GoodSecurity Penetration Test Report

ROBERTSCHMIDT@GoodSecurity.com

DATE

1/27/2022

1. High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2. Findings

Machine's IP address: 192.168.0.20

Hostname: MSEDGEWIN10

Actual name of the machine: IEUser

Vulnerability Exploited: Icecast

exploit/windows/http/icecast_header

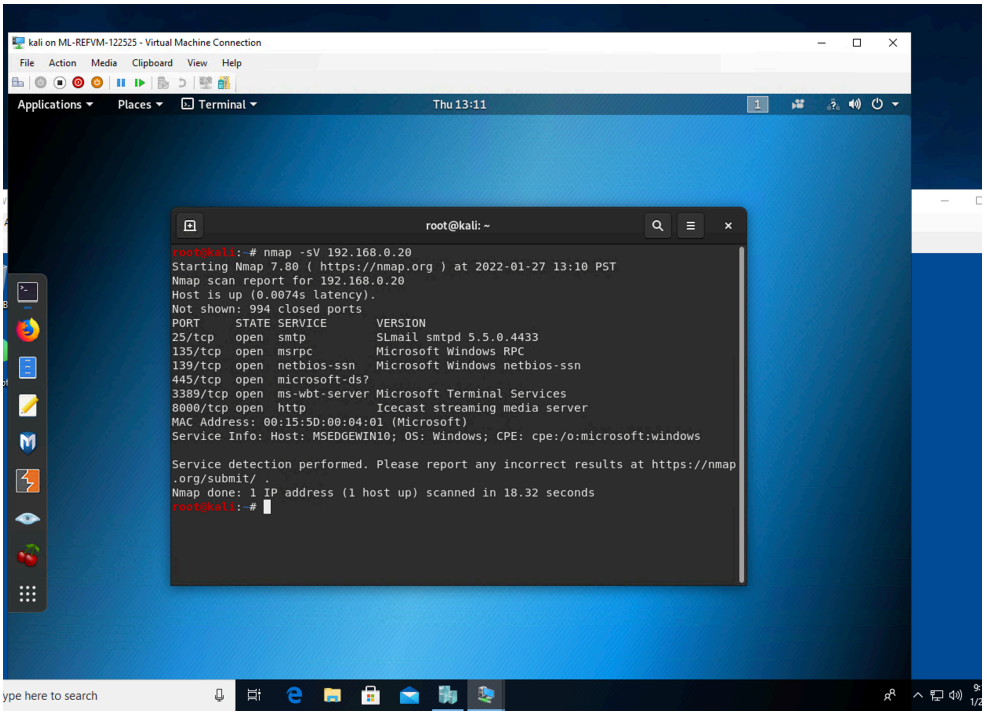
Vulnerability Explanation:

The icecast vulnerability (CVE-2004-1561) is a buffer overflow attack that allows the attacker to arbitrarily inject malicious code via an http request with a large number of headers.

Severity:The severity of this exploit is high because it allows sensitive information to be obtained. It can also have an effect on the availability of the network as it can brute force the http requests, disrupting the workflow and speed, which can affect productivity and access to the network.

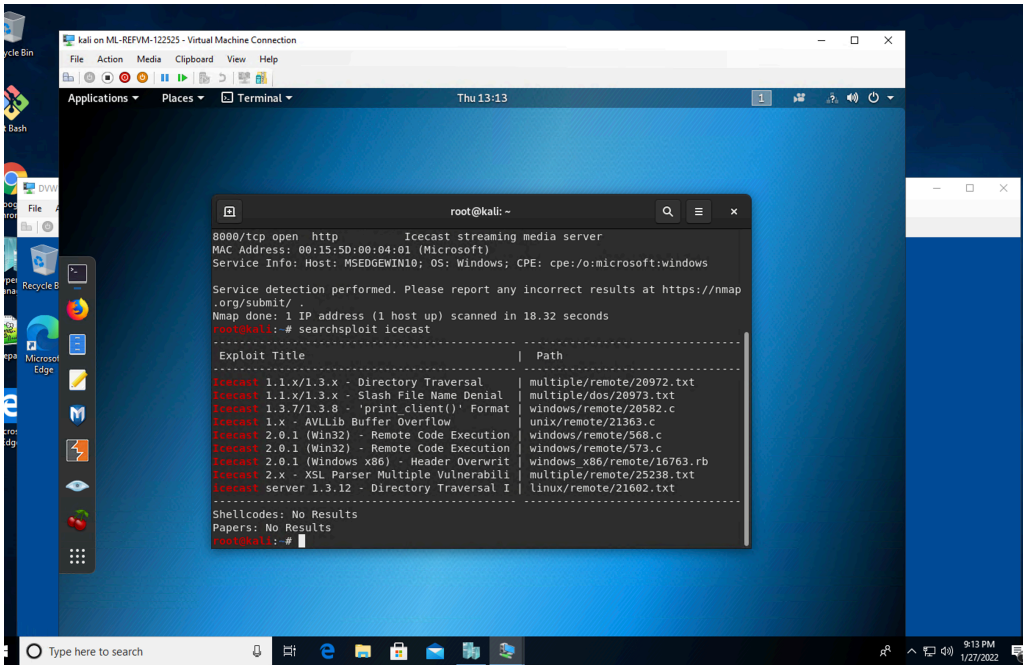
Proof of Concept:

The first step is to see what are the open ports on the target machine using Nmap:



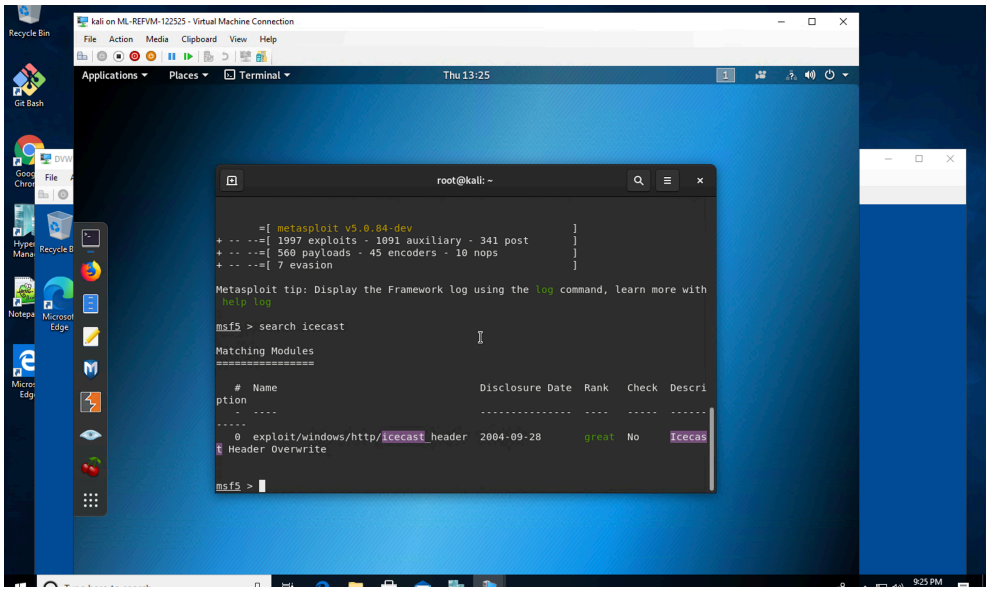
Running the Nmap scan against the IP

Then seeing that port 8000 is open and verifying that there is a vulnerability by using searchslpoit we can use it against the machine. As seen below:



Using searchsploit to find the vulnerability

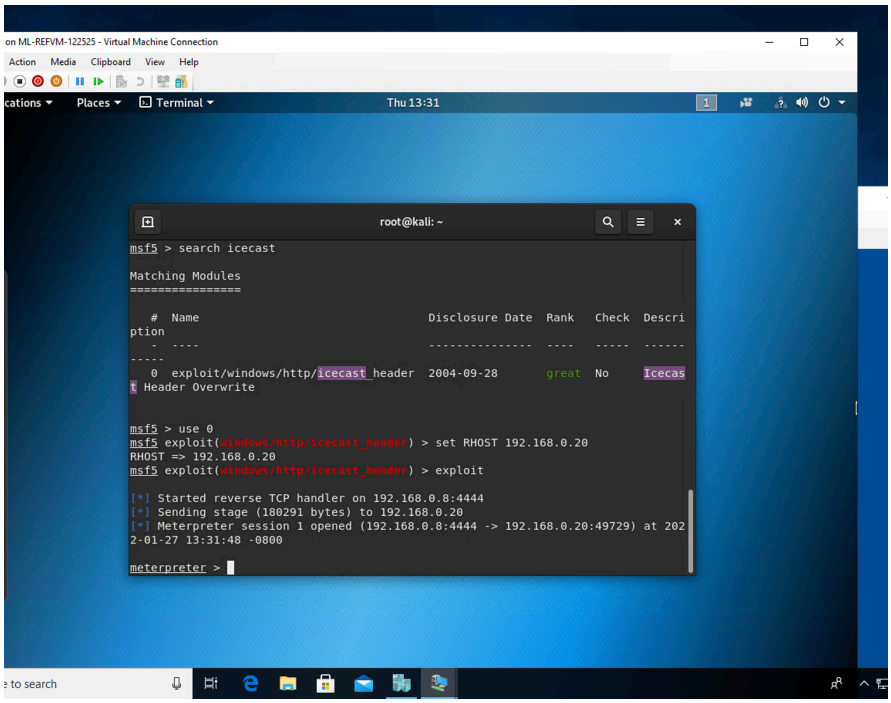
Once the vulnerability is identified we proceeded to use Metasploit to assign and execute the exploit.



Using Metasploit to verify that exploit is present

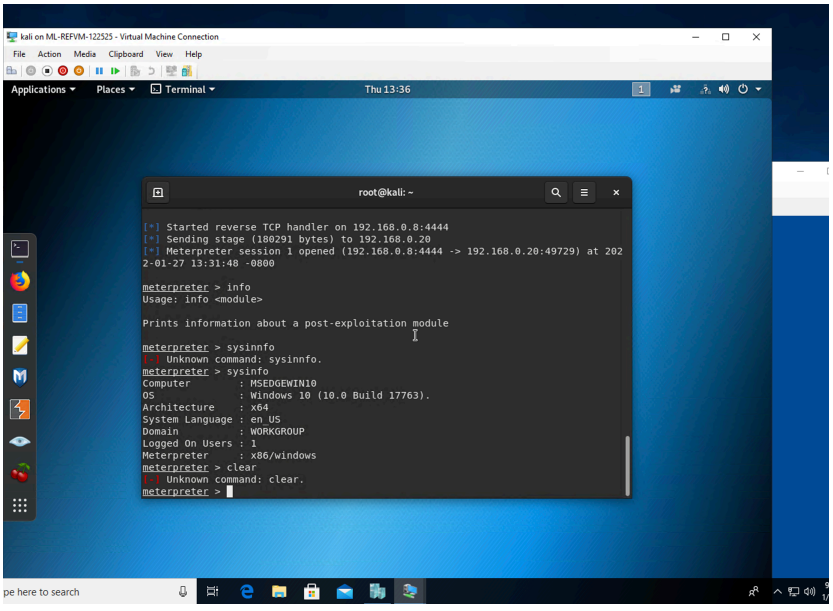
After it has been verified the exploit can be attached and delivered after setting the RHOST to the target.

The payload can then be delivered as seen below.



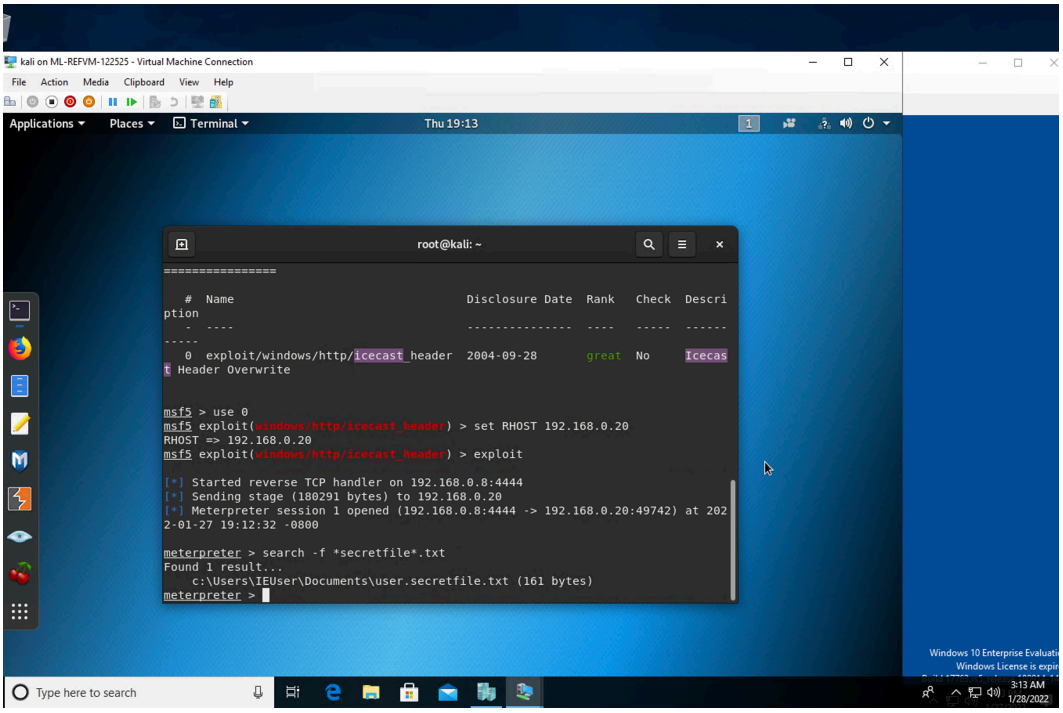
Delivering the payload via the exploit

After a session is established I ran the sysinfo to verify I was in the target machine.



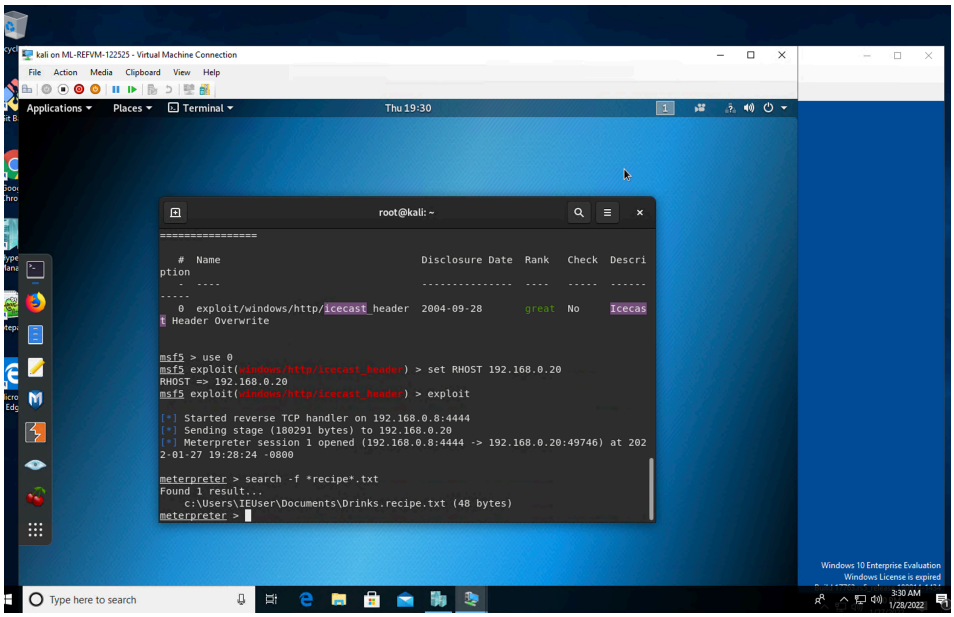
System info from target machine to verify attack

Once access was verified we located the secretfile.txt by running a search for the file.



Locating secret file with meterpreter

We also ran a search for the second file. Using the search feature once again we located the recipe.txt



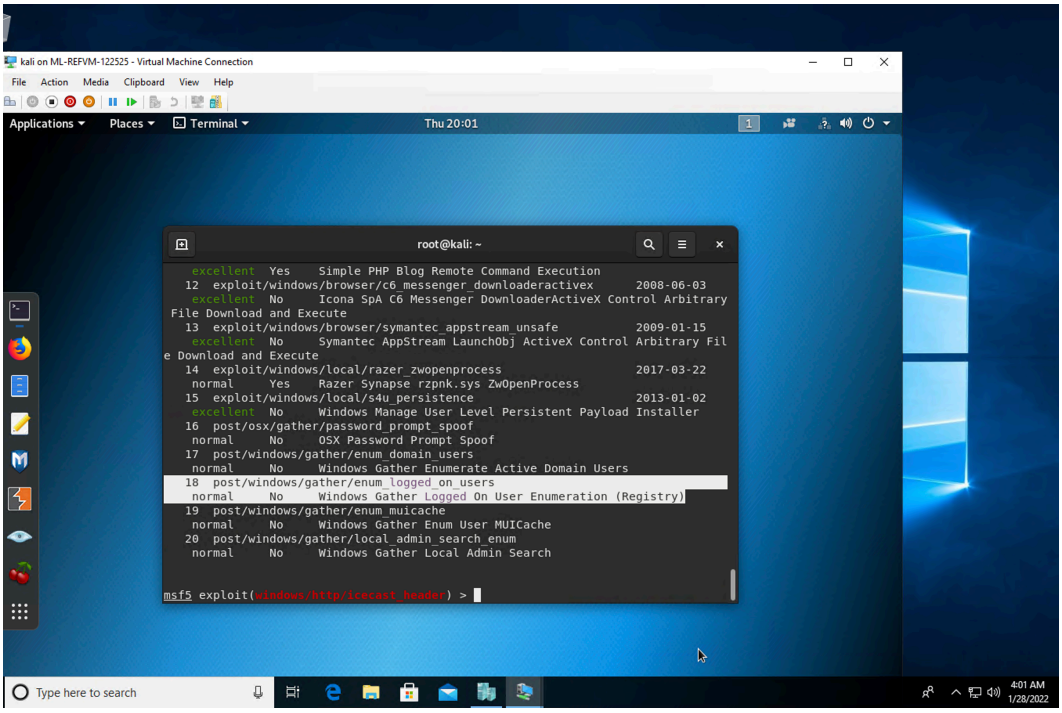
Locating the recipe file with meterpreter

3. Recommendations

In order for this vulnerability to be patched the company would need to update the icecast program to its latest version. This vulnerability cannot be utilized after a version update of at least 2.0.2 or a subsequent later update above 2.0.2.

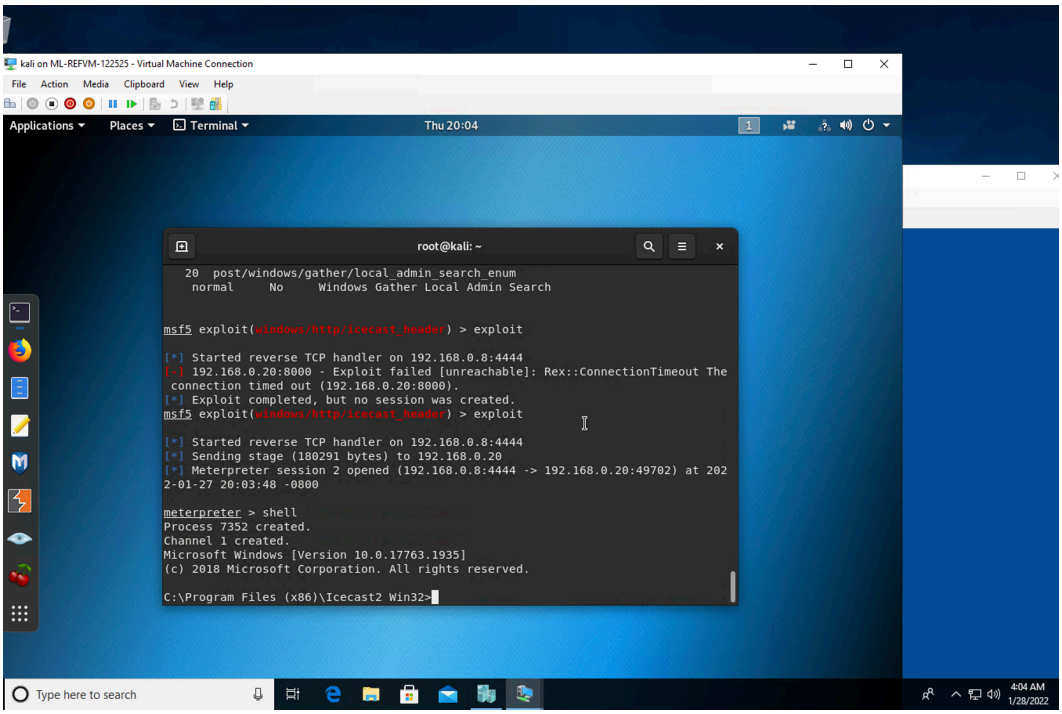
Bonus:

A. Run a Meterpreter post script that enumerates all logged on users.



Post Script for enumeration of logged users

B. Open a Meterpreter shell.



Opening of a shell

C. Run the command that displays the target's computer system information: